IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

CARSON PARKER SENEY, BRIAN MICHAEL SENEY, KARA ANN SENEY, on behalf of themselves and all others similarly situated, Plaintiffs, v. ASCENSION HEALTH, Defendant.	**Case No. _____** **CLASS ACTION COMPLAINT** **DEMAND FOR A JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiffs Carson Parker Seney, Brian Michael Seney, and Kara Ann Seney ("Plaintiffs") and on behalf of all others similarly situated, by and through undersigned counsel, bring this class action against Ascension Health ("Defendant" or "Ascension"), and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this class action lawsuit against Defendant for its failure to properly secure and safeguard Plaintiffs' and other similarly situated current and former Defendant patients' (collectively defined herein as the "Class" or "Class Members") personally identifiable information ("PII") and protected health information ("PHI"), including names, dates of birth, Social Security numbers, driver's licenses, health and health insurance information, and financial data (collectively, the "Private Information") from cybercriminals.

2. Defendant is one of the leading non-profit and Catholic health-systems that "includes 134,000 associates, 35,000 affiliated providers and 140 hospitals, serving communities

in 19 states and the District of Columbia."[1]

3. On or about May 8, 2024 Ascension detected unusual activity on its network systems which, upon further investigation, was a result of a "cybersecurity event," according to the first in a series of updates Defendant posted to its website on May 9, 2024 (the "Online Notice").[2]

4. The debilitating cyberattack severely disrupted Ascension's operations, including blocking access to systems that track and coordinate nearly every aspect of patient care, incldluing Defendant's electronic health records system, MyChart, certain phone systems, and various systems utilized to order certain tests, procedures and medications.

5. In the following weeks, Ascension admitted that the cyberattack was a ransomware attack on its servers, and cybercriminals were able to steal certain files containing its patients' PHI and PII because one of Defedant's employees downloaded a malicious file (the "Data Breach").[3]

6. A ransomware attack is a type of cybersecurity intrusion whereby the cybercriminal deploys "ransomware" on a given entity's computer system and data storage network. Ransomware is a software that works to "lock" access to a given computer system or data storage network until the entity pays a ransom, usually in untraceable cryptocurrency, in order to regain access. In this instance, Ascension has not (yet) disclosed whether it paid a ransom.

7. In fact, it appears that the Data Breach was carried out by the notorious Black Basta ransomware group, which uses the double extortion method to get its ransom – first encrypting data and then exfiltrating data and threatening to publish it if not paid. In some instances the group

---

[1] https://about.ascension.org/about-us (last visited July 3, 2024).

[2] https://about.ascension.org/cybersecurity-event (last visited July 9, 2024).

[3] *Id.*

auctions off the data rather than use it as leverage for a ransom. Black Basta "uses targeted spear-phishing attacks and exploit known vulnerabilities as an attack vector to gain initial access" to the target's systems.[4]

8. Plaintiffs' and Class Members' sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect against disclosure was targeted, compromised, and unlawfully accessed due to the Data Breach.

9. As part of its business, Defendant collects a treasure-trove of data from their patients, including highly sensitive Private Information.

10. Healthcare providers that handle Private Information have an obligation to employ reasonable and necessary data security practices to protect the sensitive, confidential and personal information entrusted to them.

11. This duty exists because it is foreseeable that the exposure of such Private Information to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, medical and financial identity theft, invasion of their private health matters and other long-term issues.

12. The harm resulting from a data and privacy breach manifests in several ways, including identity theft and financial and medical fraud, and the exposure of a person's Private Information through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives.

---

[4] *See* https://www.sangfor.com/blog/cybersecurity/black-basta-ransomware-attack-targets-ascension-healthcare

13. Mitigating that risk requires individuals to devote significant time, money and other resources to closely monitor their credit, financial accounts, health records and email accounts, as well as to take a number of additional prophylactic measures.

14. In this instance, all of that could have been avoided if Defendant had employed reasonable and appropriate data security measures.

15. As a result of the Data Breach, Defendant announced that their patients' Private Information that had been entrusted to Defendant had been compromised.[5]

16. The breach appears to have involved the divulgence of Protected Health Information (PHI) and Personally Identifiable Information (PII).[6]

17. Moreover, on information and belief, Defendant failed to mount any meaningful investigation into the breach itself, the causes, or what specific information of Plaintiffs and the proposed Class was lost to criminals.

18. Defendant's "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach has been severely diminished.

19. As a direct and proximate result of Defendant's failure to implement and to follow basic security procedures, Plaintiffs' and Class Members' PII and PHI is now in the hands of cybercriminals.

20. Plaintiffs and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of

---

[5] *See* https://about.ascension.org/cybersecurity-event (last visited July 3, 2024).

[6] *See* https://about.ascension.org/cybersecurity-event (last visited July 3, 2024).

their health privacy, Private Information being disseminated on the dark web, and similar forms of criminal mischief, risk which may last for the rest of their lives.

21. Plaintiffs and Class Members have also suffered concrete injuries in fact including, but not limited to, lost or diminished value of Private Information, lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, loss of benefit of the bargain, lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, and actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails.

22. Consequently, Plaintiffs and Class Members must devote substantially more time, money and energy to protect themselves, to the extent possible, from these crimes. *See McMorris v. Lopez*, 995 F.3d 295, 301 (2d Cir. 2021) (quoting *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.")).

23. Plaintiffs, on behalf of themself and all others similarly situated, therefore bring claims for (i) Negligence; (ii) Negligence *Per se* (iii) Breach of Implied Contract; (iv) Breach of Fiduciary Duty; (v) Invasion of Privacy; (vi) Violation of the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010 *et seq.*; (vii) Unjust Enrichment and (viii) Declaratory Judgment. Plaintiffs seek damages and injunctive relief, including the adoption of reasonably necessary and appropriate data security practices to safeguard the Private Information in Defendant's custody in order to prevent incidents like the Data Breach from occurring in the future.

PARTIES

Plaintiff Carson Paker Seney

24. Plaintiff Carson Parker Seney is a resident and citizen of Caledonia, Wisconsin and has been a patient of Ascension Health since at least 2015.

25. Plaintiff understandably and reasonably believed and trusted that his Private Information provided to Defendant would be kept confidential and secure and would be used only for authorized purposes.

Plaintiff Brian Michael Seney

26. Plaintiff Brian Michael Seney is a resident and citizen of Caledonia, Wisconsin and has been a patient of Ascension Health since 2017.

27. Plaintiff understandably and reasonably believed and trusted that his Private Information provided to Defendant would be kept confidential and secure and would be used only for authorized purposes.

Plaintiff Kara Anny Seney

28. Plaintiff Kara Ann Seney is a resident and citizen of Caledonia, Wisconsin and has been a patient of Ascension Health since 2017.

29. Plaintiff understandably and reasonably believed and trusted that her Private Information provided to Defendant would be kept confidential and secure and would be used only for authorized purposes.

Defendant Ascension Health

30. Defendant Ascension Health is a corporation organized under state laws of Missouri with its principal place of business located in St. Louis, Missouri.

JURISDICTION & VENUE

31. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members and minimal diversity exists because Plaintiffs and many putative class members are citizens of a different state than one or more Defendant.

32. This Court has jurisdiction over Defendant through its business operations in this District, the specific nature of which occurs in this District. Defendant's principal place of business is in this District. Defendant intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

33. Venue is proper in this District under 28 U.S.C. § 1391(a)(1) through (d) because: a substantial part of the events giving rise to this action occurred in this District and Defendant has harmed Class Members residing in this District.

COMMON FACTUAL ALLEGATIONS

A. Defendant Collects a Significant Amount of Private Information.

34. Plaintiffs and Class Members are current and former patients at Ascension Health.

35. Patients, including Plaintiffs and Class Members, provided Defendant with their sensitive personally identifiable information and protected health information.

36. Upon information and belief, in the course of collecting Private Information from patients, including Plaintiffs, Defendant promised to provide confidentiality and adequate security from the data it collected from patients through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

37. Defendant states on its website that: "'[T]he Site has security measures in place to

protect against the loss, misuse or alteration of information under Our control."[7]

38. Due to the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its patients, Defendant is required to keep patients' Private Information private; comply with industry standards related to data security and the maintenance of their patients' Private Information; inform their patients of its legal duties relating to data security; comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services they provide; and provide adequate notice to patients if their Private Information is disclosed without authorization.

39. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

40. Without the required submission of Private Information from Plaintiffs and Class Members, Defendant could not perform the services it provides.

41. Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

42. Defendant's actions and inactions directly resulted in the Data Breach and the compromise of Plaintiffs' and Class Members' Private Information.

B. The Data Breach

43. On or about May 9, 2024, Defendant posted a notice to its website stating the following:

---

[7] *See* https://about.ascension.org/privacy (last visited July 3, 2024).

> On Wednesday, May 8, we detected unusual activity on select technology network systems, which we now believe is due to a cybersecurity event. At this time we continue to investigate the situation. We responded immediately, initiated our investigation and activated our remediation efforts. Access to some systems have been interrupted as this process continues.
>
> Our care teams are trained for these kinds of disruptions and have initiated procedures to ensure patient care delivery continues to be safe and as minimally impacted as possible. There has been a disruption to clinical operations, and we continue to assess the impact and duration of the disruption.
>
> We have engaged Mandiant, a third party expert, to assist in the investigation and remediation process, and we have notified the appropriate authorities. Together, we are working to fully investigate what information, if any, may have been affected by the situation. Should we determine that any sensitive information was affected, we will notify and support those individuals in accordance with all relevant regulatory and legal guidelines.[8]

44. Omitted from the Online Notice were the date(s) of the Data Breach, the identity of the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

45. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

46. Moreover, in its Online Notice, Defendant failed to specify whether it undertook any efforts to contact the Class Members whose data was accessed and acquired in the Data Breach

[8] The "Online Notice". A sample copy is available at https://about.ascension.org/cybersecurity-event.

to inquire whether any of the Class Members suffered misuse of their data or whether Defendant was interested in hearing about misuse of their data or set up a mechanism for Class Members to report misuse of their data.

47. Despite Defendant's intentional opacity about the root cause of this incident, several facts may be gleaned from the Online Notice, including: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Defendant's networks and systems, and downloaded data from the networks and systems (aka exfiltrated data, or in layperson's terms "stole" data; and c) that once inside Defendant's networks and systems, the cybercriminals targeted information including, upon information and belief, Plaintiffs' and Class Members' PHI, PII, and other sensitive information for download and theft.

48. Defendant had obligations created by the FTC Act, HIPAA, contract, common law, and industry standards to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

49. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect its patients' PII and PHI.

C. Defendant Knew the Risks of Storing Valuable Private Information & the Foreseeable Harm to Victims.

50. Defendant was well aware that the Private Information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

51. Defendant also knew that a breach of its systems—and exposure of the information stored therein—would result in the increased risk of identity theft and fraud (financial and medical) against the individuals whose Private Information was compromised, as well as intrusion into their highly private health information.

52. These risks are not merely theoretical; in recent years, numerous high-profile data breaches have occurred at businesses such as Equifax, Facebook, Yahoo, Marriott, and Anthem, as well as countless ones in the healthcare industry.

53. PII has considerable value and constitutes an enticing and well-known target to hackers, who can easily sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[9]

54. PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.[10]

55. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities.

56. In 2021 alone, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[11]

57. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years; for instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[12]

---

[9] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited June 6, 2024).

[10] *See* Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited June 6, 2024).

[11] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://go.flashpoint-intel.com/docs/2021-Year-End-Report-data-breach-quickview (last visited June 6, 2024).

[12] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited

58. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[13]

59. Additionally, healthcare providers "store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it quickly – making the industry a growing target."[14]

60. Indeed, cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[15]

61. The healthcare sector suffered about 337 breaches in the first half of 2022 alone according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[16]

62. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's patients especially vulnerable to identity

---

June 6, 2024).

[13] *The healthcare industry is at risk*, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited June 6, 2024).

[14] *Id.*

[15] *2022 Breach Barometer*, https://www.protenus.com/breach-barometer-report (last visited June 6, 2024).

[16] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited June 6, 2024).

theft, tax fraud, medical fraud, credit and bank fraud and more.

63. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "[m]edical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[17]

64. A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market whereas stolen payment card information sells for about $1.[18] According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to

---

[17] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, *New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited June 6, 2024).

[18] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited June 6, 2024).

> reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[19]

65. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

66. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

67. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide

---

[19] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited June 6, 2024).

variety of fraudulent activity against Plaintiffs and Class Members.

68. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[20] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

69. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including medical identity theft, credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information.

70. For example, Social Security numbers, which were compromised in the Data Breach, are among the worst kind of Private Information to have been stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security

[20] *See* https://www.identitytheft.gov/Steps (last visited June 6, 2024).

number and assuming your identity can cause a lot of problems.[21]

71. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

72. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[22]

73. There may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused.

74. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[23]

75. Even if stolen PII or PHI does not include financial or payment card account

---

[21] *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 6, 2024).

[22] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back* (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited June 6, 2024).

[23] *Report to Congressional Requesters, Personal Information* (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited June 6, 2024).

information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

76. Based on the value of its patients' PII and PHI to cybercriminals, Defendant certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

D. The Data Breach was Preventable.

77. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

78. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

79. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented numerous measures as recommended by the United States Government, including but not limited to:

- Implementing an awareness and training program.
- Enabling strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework

(SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scanning all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configuring firewalls to block access to known malicious IP addresses.
- Setting anti-virus and anti-malware programs to conduct regular scans automatically.
- Managing the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.[24]

80. Given that Defendant was storing the Private Information of its current and former patients, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

81. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of more than eight hundred thousand individuals, including that of Plaintiffs and Class Members.

E. Defendant is Obligated Under HIPAA to Safeguard Private Information.

82. Defendant is required by HIPAA to safeguard patient PHI.

83. Defendant is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

84. HIPAA requires "compl[iance] with the applicable standards, implementation

[24] How to Protect Your Networks from RANSOMWARE, at 3, available at: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited June 7, 2024).

specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

85. Further to 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

86. Under C.F.R. 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

87. HIPAA requires Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

88. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[25]

[25] *Breach Notification Rule*, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited June 6, 2024).

89. While HIPAA permits healthcare providers to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers to disclose PHI to cybercriminals nor did Plaintiffs or the Class Members consent to the disclosure of their PHI to cybercriminals.

90. As such, Defendant is required under HIPAA to maintain the strictest confidentiality of Plaintiffs' and Class Members' PHI that it requires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

91. Given the application of HIPAA to Defendant, and that Plaintiffs and Class Members entrusted their PHI to Defendant in order to receive healthcare services, Plaintiffs and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

F. FTC Guidelines Prohibit Defendant from Engaging in Unfair or Deceptive Acts or Practices.

92. Defendant is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

93. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[26]

[26] *Start with Security – A Guide for Business* (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last

94. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[27]

95. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[28]

96. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

97. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

98. Defendant was at all times fully aware of its obligations to protect the PII and PHI of patients because of its position as a healthcare provider, which gave it direct access to reams of patient PII and PHI. Defendant was also aware of the significant repercussions that would result

visited June 6, 2024)

[27] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 6, 2024)

[28] *Id.*

from its failure to do so.

G. Defendant Violated Industry Standards.

99. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Ascension Health failed to follow these industry best practices, including a failure to implement multi-factor authentication.

100. Other best cybersecurity practices that are standard for healthcare entities include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

101. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

102. These foregoing frameworks are existing and applicable industry standards for healthcare entities, and upon information and belief, Defendant failed to comply with at least one––or all—of these accepted standards, thereby opening the door to the threat actor and causing the

Data Breach.

H. The Monetary Value of Plaintiffs' & Class Members' Private Information.

103. As a result of Defendant's failures, Plaintiffs and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their Private Information.

104. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identifying fraud is only about 3%.[29]

105. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[30]

106. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[31]

107. Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites, commonly referred to as the dark web.

108. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described

---

[29] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited June 6, 2024).

[30] *Id.*

[31] Andrew Steger, *What Happens to Stolen Healthcare Data?* (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited June 6, 2024).

the value of a consumer's personal information:

> The use of third-party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[32]

109. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[33]

110. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[34]

111. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[35] The idea is to give consumers more power and control over the type of information that they share and who

---

[32] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited June 6, 2024).

[33] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy* (Feb. 28, 2011), https://www.wsj.com/articles/SB10001424052748703529004576160764037920274 (last visited June 6, 2024).

[34] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited June 6, 2024).

[35] Angwin & Steel, *supra* note 33.

ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

112. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[36]

113. The value of Plaintiffs' and Class Members' Private Information on the black market is substantial. Sensitive health information can sell for as much as $363.[37]

114. This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

115. Health information, in particular, is likely to be used in detrimental ways—by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[38]

116. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud

---

[36] *See* U.S. Dep't of Justice, *Victims of Identity Theft* (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited June 6, 2024).

[37] *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited June 6, 2024).

[38] *Id.*

extremely dangerous."[39]

117. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[40]

118. The Federal Trade Commission has warned consumers of the dangers of medical identity theft, stating that criminals can use personal information like a "health insurance account number or Medicare number" to "see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." The FTC further warns that instances of medical identity theft "could affect the medical care you're able to get or the health insurance benefits you're able to use[,]" while also having a negative impact on credit scores.[41]

119. Here, where health insurance information was among the Private Information impacted in the Data Breach, Plaintiffs' and Class Members' risk of suffering future medical identity theft is especially substantial.

120. The ramifications of Defendant's failure to keep its patients' Private Information

---

[39] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, https://www.experian.com/innovation/thought-leadership/medical-identity-theft-healthcare-data-breaches.jsp (last visited June 6, 2024).

[40] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft/ (last visited June 6, 2024).

[41] *What to Know About Medical Identity Theft*, What To Know About Medical Identity Theft | Consumer Advice (ftc.gov) (last visited June 6, 2024).

secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for 6 to 12 months or even longer.

121. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[42] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[43]

122. Indeed, when compromised, healthcare-related data is among the most private and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[44]

123. Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft, including medical identity theft, have a crippling effect on individuals

---

[42] *See Medical ID Theft Checklist*, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited June 6, 2024).

[43] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches* (Apr. 2010), https://www.experian.com/innovation/thought-leadership/medical-identity-theft-healthcare-data-breaches.jsp (last visited June 6, 2024).

[44] Elinor Mills, *Study: Medical identity theft is costly for victims* (March 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited June 6, 2024).

and detrimentally impact the economy as a whole.[45]

124. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft (including medical identity theft) and fraud.

125. Upon information and good faith belief, had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it would have prevented the ransomware attack into their systems and, ultimately, the theft of the Private Information of patients within their systems.

126. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves.

127. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[46] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[47]

128. Based upon information and belief, the unauthorized parties have already utilized,

---

[45] *Id.*

[46] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, at 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework (last visited June 6, 2024).

[47] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

and will continue utilize, the Private Information they obtained through the Data Breach to obtain additional information from Plaintiffs and Class Members that can be misused.

129. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

130. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

131. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiffs.

132. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' Private Information has thus deprived customers of the full monetary value of their transaction with the company.

133. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

I. Plaintiffs & Class Members Have Suffered Compensable Damages.

134. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways.

135. The risks associated with identity theft, including medical identity theft, are serious.

While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

136. In order to mitigate against the risks of identity theft and fraud, Plaintiffs and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

137. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct.

138. Further, the value of Plaintiffs' and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

139. Plaintiffs and Class Members now face a greater risk of identity theft, including medical and financial identity theft.

140. Plaintiffs and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and

appropriate security and training measures to protect its patients' PII and PHI.

141. Plaintiffs and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

142. Plaintiffs and Class Members also did not receive the full benefit of their bargain when paying for medical services. Instead, they received services of a diminished value to those described in their agreements with Defendant. Plaintiffs and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

143. Plaintiffs and Class Members would not have obtained services from Defendant had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

144. Finally, in addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

REPRESENTATIVE PLAINTIFFS' EXPERIENCE

Plaintiff Carson Parker Seney

145. Plaintiff was a patient of the Defendant who started to use the Defendant's services in or around 2015.

146. As a condition of obtaining services from Defendant, he was required to provide his Private Information to Defendant.

147. Upon information and good faith belief, Defendant maintained Plaintiffs' Private Information in its systems at the time of the Data Breach.

148. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

149. Upon information and belief, Plaintiffs' Private Information was compromised in the Data Breach.

150. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services and monitoring his financial accounts for any unusual activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach – valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

151. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a)

remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

152. Plaintiff additionally suffered actual injury in the form of his Private Information being disseminated, on information and belief, on the dark web as a result of the Data Breach.

153. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

154. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

155. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Brian Michael Seney

156. Plaintiff was a patient of the Defendant who started using the Defendant's services in 2017.

157. As a condition of obtaining services from Defendant, he was required to provide his Private Information to Defendant.

158. Upon information and good faith belief, Defendant maintained Plaintiff's Private Information in its systems at the time of the Data Breach.

159. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any

other unsecured source. Plaintiff would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

160. Upon information and belief, Plaintiff's Private Information was compromised in the Data Breach.

161. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services and monitoring his financial accounts for any unusual activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach – valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

162. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

163. Plaintiff additionally suffered actual injury in the form of his Private Information

being disseminated, on information and belief, on the dark web as a result of the Data Breach.

164. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

165. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

166. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Kara Ann Seney

167. Plaintiff is a patient of the Defendant who started to use the Defendant's services back in 2017.

168. As a condition of obtaining services from Defendant, she was required to provide her Private Information to Defendant.

169. Upon information and good faith belief, Defendant maintained Plaintiff's Private Information in its systems at the time of the Data Breach.

170. Plaintiff is very careful about sharing their sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

171. Upon information and belief, Plaintiff's Private Information was compromised in the Data Breach.

172. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the

impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services and monitoring her financial accounts for any unusual activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach – valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

173. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

174. Plaintiff additionally suffered actual injury in the form of her Private Information being disseminated, on information and belief, on the dark web as a result of the Data Breach.

175. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

176. As a result of the Data Breach, Plaintiff anticipates spending considerable time and

money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

177. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

178. Plaintiffs have a continuing interest in ensuring that their Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

179. Plaintiffs bring this class action on behalf of themselves and all other individuals who are similarly situated pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

180. Plaintiffs seeks to represent a Nationwide Class of persons to be defined as follows:

> **All individuals residing in the United States whose PII and/or PHI was compromised in the Defendant's Data Breach which occurred in or about 2023 and was reported by Defendant in April 2024 (the "Nationwide Class").**

181. Plaintiffs seek to represent a Missouri Subclass of persons to be defined as follows:

> **All individuals residing in the State of Missouri whose PII and/or PHI was compromised in the Defendant's Data Breach which occurred in or about May 2024 and was reported by Defendant in 2024 (the "Missouri Subclass").**

182. Excluded from the Classes are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families, all judges assigned to hear any aspect of this litigation, their immediate family members, and those individuals who make a timely and effective election to be excluded from this matter using the correct protocol for opting out.

183. This proposed class definition is based on the information available to Plaintiffs at this time. Plaintiffs may modify the class definition in an amended pleading or when they move for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

184. **Numerosity:** Plaintiffs are informed and believe, and thereon alleges, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes many thousands of individuals, if not substantially more.

185. **Commonality:** This action involved questions of law and fact common to the Class that predominate over any questions affecting solely individual members of the Class. Such common questions include but are not limited to:

a. Whether Defendant failed to timely notify Plaintiffs and Class Members of the Data Breach;

b. Whether Defendant had a duty to protect the PII and PHI of Plaintiffs and Class Members;

c. Whether Defendant had respective duties not to disclose the PII and PHI of Plaintiffs and Class Members to unauthorized third parties;

d. Whether Defendant had respective duties not to disclose the PII and PHI of Plaintiffs and Class Members for non-business purposes;

e. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiffs and Class Members;

f. Whether and when Defendant actually learned of the Data Breach;

g. Whether Defendant was negligent in collecting and storing Plaintiffs' and Class Members' PII and PHI, and breached its duties thereby;

h. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;

i. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII and PHI had been compromised;

j. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

k. Whether Defendant adequately addressed and fixed the vulnerabilities that allowed the Data Breach to occur;

l. Whether Defendant was negligent and that negligence resulted in the Data Breach;

m. Whether Defendant entered into an implied contract with Plaintiffs and Class Members;

n. Whether Defendant breached that contract by failing to adequately safeguard Plaintiffs' and Class Members' PII and PHI;

o. Whether Defendant were unjustly enriched;

p. Whether Plaintiffs and Class Members are entitled to actual, statutory, and/or nominal damages as a result of Defendant's wrongful conduct; and

q. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

186. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class.

The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and members of the Class were all patients, or family members or caregivers of patients, of Defendant, each having their PII and PHI exposed and/or accessed by an unauthorized third party.

187. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenges of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

188. **Adequacy of Representation:** Plaintiffs are an adequate representative of the Class because their interests do not conflict with the interests of the members of the Class. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and have no interests antagonistic to the members of the Class. In addition, Plaintiffs has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiffs and the Class Members are substantially identical as explained above.

189. **Superiority and Manageability:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision

by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

190. Class action Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

191. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

192. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

193. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

194. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

195. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

196. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiffs and the class of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard patient Private Information; and Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

197. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the Class. If Defendant breached its duty to Plaintiffs and Class Members, then Plaintiffs and each Class member suffered damages by that conduct.

198. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

199. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's books and records.

CAUSES OF ACTION

COUNT I
Negligence
(On behalf of Plaintiffs & the Nationwide Class)

200. Plaintiffs restate and reallege all preceding factual allegations above as if fully set forth herein.

201. Plaintiffs bring this claim individually and on behalf of the Class.

202. Defendant owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

203. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

204. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By collecting and storing valuable PII and PHI that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

205. Defendant's duty also arose from Defendant's position as healthcare provider. Defendant holds itself out as trusted providers of healthcare, and thereby assumes a duty to reasonably protect its patients' information. Indeed, Defendant was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

206. Defendant breached the duties owed to Plaintiffs and Class Members and thus were negligent. As a result of a successful attack directed towards Defendant that compromised Plaintiffs' and Class Members' PII and PHI, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the

sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to their patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

207. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII and PHI would not have been compromised.

208. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection

services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members;

j. The diminished value of the services they paid for and received, and

k. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

209. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT II
Negligence *Per Se*

(On Behalf of Plaintiffs and the Class)

210. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

211. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

212. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

213. Defendant breached its duties to Plaintiffs and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

214. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se.*

215. Plaintiffs and Class Members are within the class of persons the statutes were intended to protect and the harm to Plaintiffs and Class Members resulting from the Data Breach was the type of harm against which the statutes were intended to prevent.

216. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

217. The injury and harm suffered by Plaintiffs and Class Members was the reasonably

foreseeable result of Defendants' breach of their duties. Defendant knew or should have known that by failing to meet its duties, Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

218. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(On behalf of Plaintiffs & the Nationwide Class)

219. Plaintiffs restate and reallege all preceding factual allegations above as if fully set forth herein.

220. Plaintiffs bring this claim individually and on behalf of the Class.

221. When Plaintiffs and Class Members provided their PII and PHI to Defendant, they entered into implied contracts with Defendant, under which Defendant agreed to take reasonable steps to protect Plaintiffs' and Class Members' PII and PHI, comply with their statutory and common law duties to protect Plaintiffs' and Class Members' PII and PHI, and to timely notify them in the event of a data breach.

222. Defendant solicited and invited Plaintiffs and Class Members to provide their PII and PHI as part of Defendant's provision of healthcare services. Plaintiffs and Class Members accepted Defendant's offers and provided their PII and PHI to Defendant.

223. Implicit in the agreement between Plaintiffs and Class Members and Defendant, was Defendant's obligation to: (a) use such PII and PHI for business purposes only; (b) take reasonable steps to safeguard Plaintiffs' and Class Members' PII and PHI; (c) prevent unauthorized access and/or disclosure of Plaintiffs' and Class Members' PII and PHI; (d) provide Plaintiffs and

Class Members with prompt and sufficient notice of any and all unauthorized access and/or disclosure of their PII and PHI; (e) reasonably safeguard and protect the PII and PHI of Plaintiffs and Class Members from unauthorized access and/or disclosure; and (f) retain Plaintiffs' and Class Members' PII and PHI under conditions that kept such information secure and confidential.

224. When entering into implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with their statutory and common law duties to adequately protect Plaintiffs' and Class Members' PII and PHI and to timely notify them in the event of a data breach.

225. Plaintiffs and Class Members paid money to Defendant in exchange for services, along with Defendant's promise to protect their PII and PHI from unauthorized access and disclosure. Plaintiffs and Class Members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

226. Plaintiffs and Class Members would not have provided their PII and PHI to Defendant had they known that Defendant would not safeguard their PII and PHI, as promised, or provide timely notice of a data breach.

227. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

228. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard their PII and PHI and by failing to provide them with timely and accurate notice of the Data Breach

229. The losses and damages Plaintiffs and Class Members sustained, include, but are not limited to:

a. Theft of their PII and/or PHI;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members;

j. The diminished value of the services they paid for and received; and

k. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

230. As a direct and proximate result of Defendant's breach of contract, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

231. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (1) strength its data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) immediately provide and continue to provide adequate credit monitoring to Plaintiffs and all Class Members.

COUNT III
Breach of Fiduciary Duty
(On behalf of Plaintiffs & the Nationwide Class)

232. Plaintiffs restate and reallege all preceding factual allegations above as if fully set forth herein.

233. Given the relationship between Defendant and Plaintiffs and Class members, where Defendant became guardian of Plaintiffs' and Class members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiffs and Class members, (1) for the safeguarding of Plaintiffs and Class members' PII/PHI; (2) to timely notify Plaintiffs and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

234. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

235. Because of the highly sensitive nature of the PII/PHI, Plaintiffs and Class members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

236. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class members' PII/PHI.

237. Defendant also breached its fiduciary duties to Plaintiffs and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

238. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

COUNT IV
Invasion of Privacy
(On behalf of Plaintiffs & the Nationwide Class)

239. Plaintiffs restate and reallege all preceding factual allegations above as if fully set forth herein.

240. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

241. Defendant owed a duty to its current and former patients, including Plaintiffs and

the Class, to keep this information confidential.

242. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class members' PII/PHI is highly offensive to a reasonable person.

243. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

244. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

245. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

246. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

247. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

248. As a proximate result of Defendant's acts and omissions, the private and sensitive PII/PHI of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

249. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

250. Unless and until enjoined and restrained by order of this Court,

251. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII/PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

252. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiffs and the Class.

253. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT V
Violation of the Missouri Merchandising Practices Act,
Mo. Rev. Stat. § 407.010 *et seq.*
(On behalf of Plaintiffs & the Missouri Subclass)

254. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

255. The Missouri Merchandising Practice Act (the "MMPA") prohibits false, fraudulent, or deceptive merchandising practices to protect both consumers and competitors by promoting fair competition in commercial markets for goods and services.

256. The MMPA prohibits the "act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice, or the concealment,

suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce." Mo. Rev. Stat. § 407.020.

257. The MMPA defines "Merchandise" as "any objects, wares, goods, commodities, intangibles, real estate or services." Mo. Rev. Stat. § 407.010(4).

258. Plaintiff, individually and on behalf of the Class, is entitled to bring an action pursuant to Mo. Rev. Stat. § 407.025, which provides in relevant part that: (a) Any person who purchases or leases merchandise primarily for personal, family or household purposes and thereby suffers an ascertainable loss of money or property, real or personal, as a result of the use or employment by another person of a method, act or practice declared unlawful by section 407.20, may bring a private civil action in either the circuit court of the county in which the seller or lessor resides or in which the transaction complained of took place, to recover actual damages. The court may, in its discretion, award the prevailing party attorneys' fees, based on the amount of time reasonably expended, and may provide such equitable relief as it deems necessary or proper. Mo. Rev. Stat. § 407.025.

259. Defendant is a "person" within the meaning of the MMPA in that Defendant is a domestic, for-profit corporation. Mo. Rev. Stat. § 407.010(5).

260. Plaintiffs and Class Members are "persons" under the MMPA because they are natural persons and they used Defendant's services for personal, family, and/or household use.

261. The Missouri Attorney General has specified the settled meanings of certain terms used in the enforcement of the MMPA. Specifically, Mo. Code Regs. tit. 15, § 60-8.020, provides:

(1) Unfair practice in any practice which—

a. Either—

i. Offends any public policy as it has been established by the

Constitution, statutes, or common law of this state, or by the Federal Trade Commission, or its interpretative decisions; or

ii. Is unethical, oppressive, or unscrupulous; and

b. Presents a risk of, or causes, substantial injury to consumers.

262. Proof of deception, fraud, or misrepresentation is not required to prove unfair practices as used in section 407.020.1, RSMo. (*See Federal Trade Commission v. Sperry and Hutchinson Co.*, 405 U.S. 233, 92 S. Ct. 898, 31 L.Ed.2d 170 (1972); *Marshall v. Miller*, 302 N.C. 539, 276 S.E.2d 397 (N.C. 1981); *see also*, Restatement, Second, Contracts, sections 364 and 365. Defendant offered and continues to offer healthcare and other related services in the State of Illinois.

263. Pursuant to the MMPA and Mo. Code Regs. Tit. 15, § 60- 8.020, Defendant's acts and omissions fall within the meaning of "unfair."

264. Defendants engaged in a "trade" or "commerce" within the meaning of the MMPA with regard to services which are supposed to keep Plaintiffs' and the Class Members's Private Information safe and secure.

265. Defendant engaged in unlawful practices and deceptive conduct, which emanated from its Missouri headquarters, in violation of the MMPA by omitting and/or concealing material facts related to the safety and security of Plaintiffs' and the Class Members's Private Information. Defendant's unfair and unethical conduct of failing to secure Private Information and failing to disclose the Data Breach caused substantial injury to consumers in that the type of consumers' personal information impacted by the breach can be used to orchestrate a host of fraudulent activities, including medical, insurance, and financial fraud and identity theft. The impacted consumers have been placed in an immediate and continuing risk of harm from fraud, identity

theft, and related harm caused by the Data Breach.

266. Defendant's conduct of failing to secure data required Plaintiffs and the Class to undertake time-consuming, and often costly, efforts to mitigate the actual and potential harm caused by the Data Breach's exposure of their Private Information.

267. Defendant's conduct of concealing, suppressing, or otherwise omitting material facts regarding the Data Breach was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the MMPA.

268. By failing to secure sensitive data and failing to disclose and inform Plaintiffs and Class Members about the Breach of Private Information, Defendant engaged in acts and practices that constitute unlawful practices in violation of the MMPA. Mo. Ann. Stat. §§ 407.010, *et seq.*

269. Defendant engaged in unlawful practices and deceptive conduct in the course of their business that violated the MMPA including misrepresentations and omissions related to the safety and security of Plaintiffs' and the Class's Private Information. Mo. Rev. Stat. § 407.020.1.

270. As a direct and proximate result of these unfair and deceptive practices, Plaintiffs and each Class member suffered actual harm in the form of money and/or property because the disclosure of their Private Information has value encompassing financial data and tangible money.

271. Defendant's "unfair" acts and practices include:

a. by utilizing cheaper, ineffective security measures and diverting those funds to its own profit, instead of providing a reasonable level of security that would have prevented the hacking incident;

b. failing to follow industry standard and the applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data;

c. failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages;

d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' personal information; and

e. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA.

272. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' personal information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' personal information, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA.

273. Defendant's misrepresentations and omissions were material to consumers and made in order to induce consumers' reliance regarding the safety and security of Private Information in order to obtain consumers' Private Information and purchase of medical products and/or services.

274. Defendant's deceptive practices misled Plaintiffs and the Class and would cause a reasonable person to enter into transactions with Defendant that resulted in damages.

275. As such, Plaintiffs and the Class seek: (1) to recover actual damages sustained; (2) to recover punitive damages; (3) to recover reasonable attorneys' fees and costs; and (4) such equity relief as the Court deems necessary or proper to protect Plaintiffs and the members of the Class from Defendant's deceptive conduct and any other statutorily available damages or relief the court deems proper.

COUNT VI
Unjust Enrichment
(*On behalf of Plaintiffs & the Nationwide Class*)

276. Plaintiffs restate and reallege all preceding factual allegations above as if fully set forth herein and pleads the following count in the alternative.

277. Plaintiffs bring this claim individually and on behalf of the Class.

278. Upon information and belief, Defendant funded its data security measures from its general revenue including payments made by or on behalf of Plaintiffs and Class Members.

279. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion

of each payment made that is allocated to data security is known to Defendant.

280. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased healthcare services from Defendant and/or their agents and in so doing provided Defendant with their PII and PHI.

281. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII and PHI protected with adequate data security.

282. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII and PHI of Plaintiffs and Class Members for business purposes.

283. In particular, Defendant enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members PII and PHI. Instead of providing a reasonable level of data security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits and the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective data security measures.

284. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to implement appropriate data management and security measures that are mandated by their common law and statutory duties.

285. Defendant failed to secure Plaintiffs and Class Members' PII and PHI and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members conferred upon Defendant.

286. Defendant acquired Plaintiffs' and Class Members' PII and PHI through

inequitable means in that it failed to disclose the inadequate security practices previously alleged.

287. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendant.

288. Plaintiffs and Class Members have no adequate remedy at law.

289. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members;

j. The diminished value of the services they paid for and received; and

k. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

290. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

291. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

COUNT VII
Declaratory Judgment and Injunctive Relief
(On behalf of Plaintiffs & the Nationwide Class)

148. Plaintiffs restate and reallege all preceding allegations above as if fully set forth herein.

149. Plaintiffs bring this claim individually and on behalf of the Class.

150. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

151. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs' and Class Members from further data breaches that compromise their PII and PHI. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and PHI and remains at imminent risk that further compromises of their PII and PHI will occur in the future.

152. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure patients' PII and PHI and to timely notify patients of a data breach under the common law, Section 5 of the FTC Act, and HIPAA; and

b. Defendant continues to breach this legal duty by failing to employ reasonable

measures to secure patients' PII and PHI.

153. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect patients' PII and PHI.

154. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant's properties.

155. The risk of another such breach is real, immediate and substantial.

156. If another breach of Defendant's store of patient data occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

157. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

158. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Defendant [what], thus eliminating the additional injuries that would result to Plaintiffs and Class Members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and other Class Members, pray for judgment against Defendant as follows:

A. an Order certifying the Nationwide Class, and appointing Plaintiffs and

their Counsel to represent the Class;

B. equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

C. injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

D. an award of all damages available at equity or law, including, but not limited to, actual, consequential, punitive, statutory and nominal damages, as allowed by law in an amount to be determined;

E. an award of attorney fees, costs, and litigation expenses, as allowed by law;

F. prejudgment interest on all amounts awarded and

G. all such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and other members of the proposed Classes, hereby demands a jury trial on all issues so triable.

Dated: July 9, 2024

Respectfully Submitted,

/s/ Brandon M. Wise
Brandon M. Wise (MO Bar. #67242)
PEIFFER WOLF CARR
KANE CONWAY & WISE, LLP
One US Bank Plaza, Suite 1950
St. Louis, MO 63101
Ph: (314) 833-4825
bwise@peifferwolf.com

David S. Almeida*
IL Bar # 6285557

ALMEIDA LAW GROUP LLC
Firm ID 100530
849 W. Webster Avenue
Chicago, Illinois 60614
(312) 576-3024 (phone)
david@almeidalawgroup.com

**pro hac vice to be sought*

Attorneys for Plaintiffs and the Classes